(12) UK Patent Application (19) GB (11) 2 405 007 (13) A

(43) Date of A Publication 16.02.2005

(21) Application No: 0423668.3

(22) Date of Filing: 19.07.2002

Date Lodged: 22.10.2004

(62) Divided from Application No
0216770.8 under Section 15(4) of the Patents Act 1977

(71) Applicant(s):
**RiTech International Limited
(Incorporated in Hong Kong)
Unit 919, New Commerce Centre,
19 On Sum Street, Siu Lek Yuen,
New Territories, Hong Kong**

(72) Inventor(s):
Boon Lum Lim

(continued on next page)

(51) INT CL^7:
G06F 1/00 // G06F 12/14 , H04L 9/30

(52) UK CL (Edition X):
G4A AAP

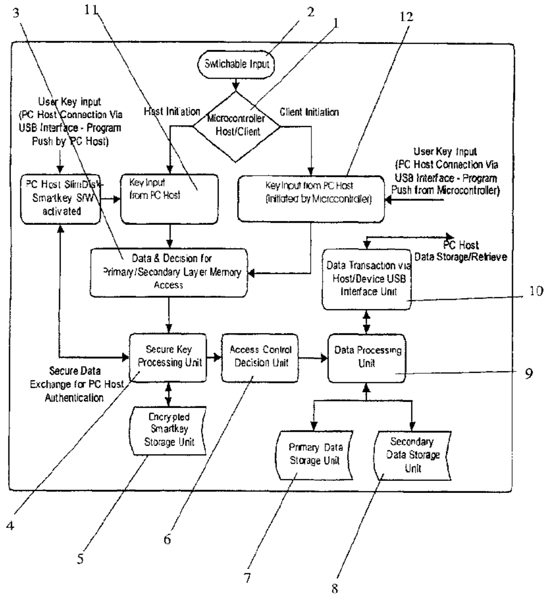
(56) Documents Cited:
GB 2387933 A **EP 0673134 A2**

(58) Field of Search:
UK CL (Edition W) **G4A**
INT CL^7 **G06F, H04L**
Other: **WPI, EPODOC, PAJ, INSPEC, XPESP, IP.COM, IEL, Internet, TDB**

(54) Abstract Title: **Process of encryption and decryption of data in a portable data storage device with layered memory architecture**

(57) A process of encryption and decryption of data held in a portable data storage device where the user key to access the data is converted to an encrypted pseudo random generated key which is then combined with a factory preset key in a polynominal process to produce a secure key.

FIGURE 1


3
11
2
1
12
Swtichable Input
User Key input (PC Host Connection Via USB Interface - Program Push by PC Host)
Host Initiation
Microcontroller Host/Client
Client Initiation
User Key Input (PC Host Connection Via USB Interface - Program Push from Microcontroller)
PC Host SlimDisk Smartkey S/W activated
Key Input from PC Host
Key Input from PC Host (initiated by Microcontroller)
PC Host Data Storage/Retrieve
Data & Decision for Primary/Secondary Layer Memory Access
Data Transaction via Host/Device USB Interface Unit
10
Secure Key Processing Unit
Access Control Decision Unit
Data Processing Unit
9
Secure Data Exchange for PC Host Authentication
Encrypted Smartkey Storage Unit
Primary Data Storage Unit
Secondary Data Storage Unit
4
5
6
7
8

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

This print takes account of replacement documents submitted after the date of filing to enable the application to comply with the formal requirements of the Patents Rules 1995

GB 2405007 A continuation

(74) Agent and/or Address for Service:
M Grewal & Co
45 Berkeley Avenue, Cranford,
HOUNSLOW, Middlesex, TW4 6LE,
United Kingdom

FIGURE 1

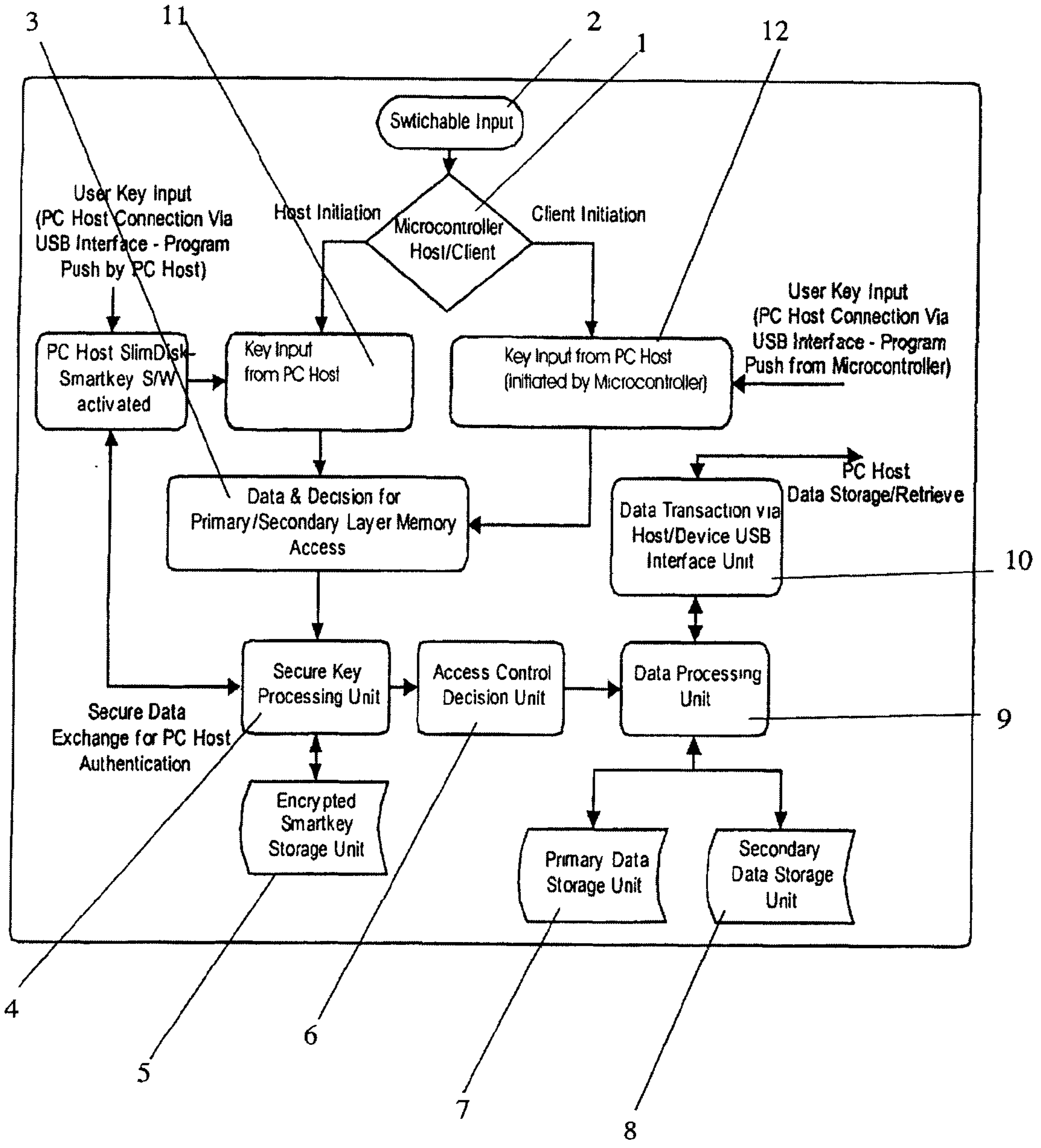
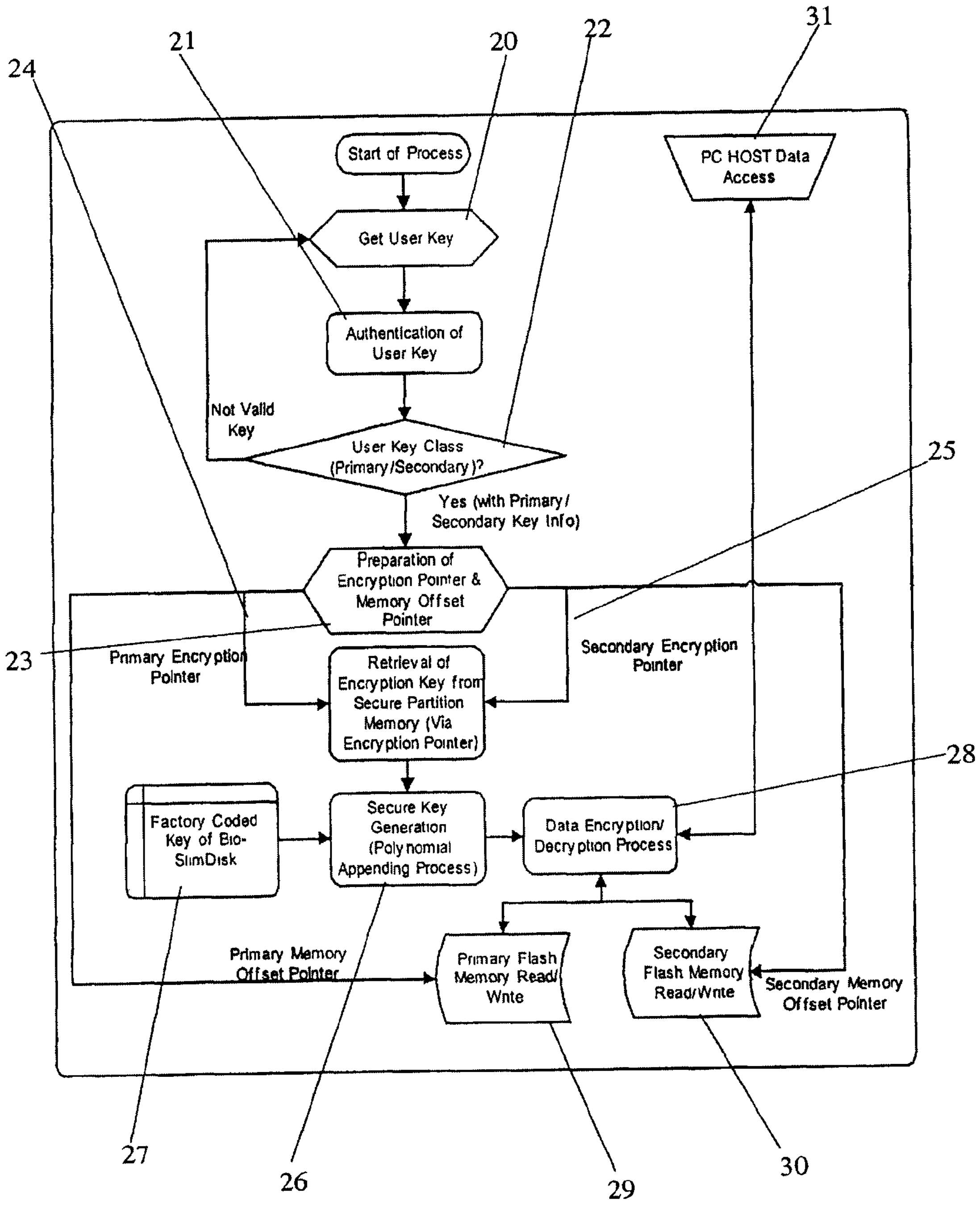

3
11
2
1
12
Swtichable Input
Microcontroller Host/Client
Host Initiation
Client Initiation
User Key Input (PC Host Connection Via USB Interface - Program Push by PC Host)
PC Host SlimDisk-Smartkey S/W activated
Key Input from PC Host
Key Input from PC Host (initiated by Microcontroller)
User Key Input (PC Host Connection Via USB Interface - Program Push from Microcontroller)
Data & Decision for Primary/Secondary Layer Memory Access
PC Host Data Storage/Retrieve
Data Transaction via Host/Device USB Interface Unit
10
Secure Key Processing Unit
Access Control Decision Unit
Data Processing Unit
9
Secure Data Exchange for PC Host Authentication
Encrypted Smartkey Storage Unit
Primary Data Storage Unit
Secondary Data Storage Unit
4
5
6
7
8

FIGURE 2



31
24
21
20
22
Start of Process
PC HOST Data Access
Get User Key
Authentication of User Key
Not Valid Key
User Key Class (Primary/Secondary)?
Yes (with Primary/ Secondary Key Info)
25
Preparation of Encryption Pointer & Memory Offset Pointer
23
Pnmary Encryption Pointer
Secondary Encryption Pointer
Retrieval of Encryption Key from Secure Partition Memory (Via Encryption Pointer)
28
Factory Coded Key of Bio-SlimDisk
Secure Key Generation (Polynomial Appending Process)
Data Encryption/ Decryption Process
Primary Memory Offset Pointer
Primary Flash Memory Read/ Wnte
Secondary Flash Memory Read/Wnte
Secondary Memory Offset Pointer
27
26
29
30

2405007

PROCESS OF ENCRYPTION & DECRYPTION OF DATA IN A PORTABLE DATA STORAGE DEVICE WITH LAYERED MEMORY ARCHITECTURE

This is a divisional application of patent application number GB 0216770.8, filed on 19th July2002 and published on 28th January2004 under application number GB 2 391 082.

The application herein relates solelyto the process of encryption and decryption of data held in a portable data storage device with layered memory architecture as disclosed in the aforesaid application.

In a portable data storage device as disclosed in the aforesaid application there is provided a means wherein the device can act as a host i.e. the enrolled user can input the keyto access the data directly into the device, or the device can act a client in respect of access to the data i.e. the enrolled user can input the keyinto host computer to which the device is attached in order to access the data and where the data is stored in layered memory architecture providing a secure primary and secondary partition structure. In such a device there is further provided a means of data encryption for keeping data secure and decryption to provide authorised users access to the data.

The aforesaid invention provides a data storage disk disposed with a communications interface and host/client switchable technology to create a novel architecture and communications protocol to ensure data stored in the disk is secured using data encryption process. The architecture provides the user with layer protection which employs a self initiated host/client switchable controller which secures access not only to the data but also access to any host computer to which the disk is attached.

Data stored within the disk is secured by means of memory partition architecture and data protection protocol and procedure such that data within the memory storage is layered and encrypted using encryption technology. As a consequence of such security it would be impossible for any one to access the data without the primary key input.

The data storage disk is disposed with:

1. A communications interface;
2. A microcontroller with built in switchable input;
3. a primary and secondary memory storage means;
4. A data processing unit;
5. Data and decision means;
6. Secure key processing unit;
7. An access control decision unit;
8. An encrypted smart key storage unit.

The communications interface which may be a USB type interface or other communications interface permits users to access the data stored in the memory means of the device. The communications interface enables a user to reversibly access the data in the storage disk.

The microcontroller is disposed with a switchable input interconnected to a data and decision means for primary and secondary layer memory access. The microcontroller and data and decision means are responsible for interfacing between a host computer and the memory storage means and as such provide a gateway for data storage and retrieval and the processing in and from the flash memory means for authorised users.

The primary and secondary storage means are used to store data to permit selective access to users in accordance with the authorization granted to the user and access to such data is secured byreference to a secure encrypted key

The switchable input can be initiated by a host computer to which the device is attached wherein the device acts as a client or the input can be initiated by the microcontroller itself wherein the device acts as a host. Key input can be made from the host computer or directly from the device itself. Such key input can then be analysed by the data and decision means for access to primary and secondary layer memory.

The secure key processing unit is reversibly interconnected with an encrypted smart key storage unit and is further connected to the access control decision unit. The access control decision unit is connected to the data processing unit.

The data processing unit is in two way communication with a primary and secondary flash memory means and is accessed by the and interconnected with the communications interface. The data processing unit permits two way access to the layered memory means.

To access the data held in the memory means a user, who must firstly be enrolled, is obliged to input his/her key directly to the device or to a host computer to which the device is connected. By permitting such switchable input access control it enables the user of the device to permit authorised third parties to access the data held in the device via an approved computer host device.

The input key is converted to a pseudo random generated key by means of encryption technology. This encrypted user input key is stored in the memory means. To this encryption key the secure key processing unit adds a factory preset code in a polynominal appending process to produce a secure key. Thus the secure polynominal key is based on a user input key and a factory preset code. This secure encrypted polynominal key is stored in the memory means.

Access to the data requires the user to input the appropriate user key input either through the device or through an approved host computer to which the device is attached. Authentication of the input key permits the user to proceed to encryption key generation procedure and primary and secondary memory access.

Enrollment of users requires users to input a keyof their own choice either directly to the device or via the host computer to which the device is attached. The user key is encrypted by reference to pseudo random generated parameters and stored in the memory means. This encrypted key is then combined with a factory preset code to form a secure polynominal key. Such key is pointed and is accessible by a key known as an encryption pointer. User access can be selectively restricted either the primary or secondary memory layer or to both layers.

To access data the user will input his/her input key. The data and decision means for access to the primary and/or secondary layer memory authenticates the user input. An encryption pointer is then prepared by to retrieve the encryption key from the secure partition memory. The encryption key is then combined with the factory preset key to generate a secure polynominal key. This polynominal key is then decrypted by the secure key processing unit. The access control decision unit then grants access to the data which is processed by the data processing unit.

By partitioning the memory means it is possible to selectively restrict access that users may have to the data held in storage. This is achieved by means of layered encryption architecture. The highest level of authorisation would permit the user to all the data stored in the different memory partitions while lower level of authorisation would restrict access to data held in one or other partition layer. It is thus possible to enable a user to permit third parties to access some or all of the data held in the device through selective enrollment procedure. Such third party users would be able to access the data through an authorised host computer by inputting their user key.

The invention will now be described by reference to the drawings.

Figure 1 is a block diagram of the system components.

Figure 2 is a flowchart of the key encryption scheme for access to the primary and secondary memory means.

Figure 1 is a block diagram of the system components. The device is disposed with a communications interface (10) which links the device to a host computer and which is in two way communication with a data processing unit (9). The data processing unit is in communication with an access control decision unit (6) and the primary data storage unit (7) and the secondary data storage unit (8). The access control decision unit is in communication with and receives input from the secure key processing unit (4).

The secure key processing unit is in two way communication with the encrypted smart key storage unit (5) and is also in communication with and receives input from the data and decision means (3) for access to the primary and/or secondary layer memory means and the communications interface.

The data and decision means (3) is in communication with and receives key input from the host computer (11) and/or key input from the device itself (12). The key input is in communication with a micro controller (1) which is in communication with a switchable input (2).

Figure 2 shows the flow chart of key encryption scheme to access the memory means. At the start of the process the user inputs his/her key input (20). This user key input is then authenticated (21) by the data and decision means (3). The user key input is then evaluated to determine whether the user is entitled to primary and/or secondary level memory access (22). This process is also carried out by the data and decision means (3).

Once the use key input has been authenticated and its access class determined an encryption pointer key is prepared (23). The encryption key in respect of enrolled users is retrieved from the secure memory means (24) for primary level access and (25) for secondary level access by preparing a primary or secondary encryption pointer key. A secure key is then generated (26) by the secure key processing unit (4) by a polynominal appending process in which the factory encrypted key (27), stored in the encrypted smart key storage unit (5) and the encrypted user key input are combined.

This secure key is then decrypted (28) by the data processing unit (9) to permit the user access to the primary (29) and/or the secondary (30) level memory means. The data can then be accessed via the communications interface (10) linked to a host computer (31).

CLAIMS

1. A process of encryption in a data storage device which can interface with a computer such as a desktop PC or a mobile portable notebook computer and which can secure data by a process of encryption and wherein the data stored in the device is stored in layered memory architecture and wherein the device is disposed with a communications interface, a microcontroller with a built in switchable input means, a primary and secondary memory storage means, a data processing unit, a data and decision means, a secure key processing unit, an access control decision unit and an encryption smart key storage unit and wherein key input to access the data can be via the host computer to which the device is attached or via the device itself wherein the device acts as the host and wherein key input by the user to access the data is converted to an encrypted pseudo random generated key in accordance with predefined algorithms and wherein this encrypted key is combined with a factory preset key in a polynomial sequence appending process to produce a secure keyand wherein the secure key is pointed and is only accessible by an encryption pointer key.

2. A process of encryption as claimed in claim 1 above wherein the secure encrypted polynomial key is stored in the memory means.

3. A process of decryption of key input by a user wherein the key input is evaluated and authenticated by the data and decision means and upon authentication an encryption pointer is prepared

by the key processing unit to retrieves the secure encryption key from the secure memory means and wherein a secure key is generated by the secure key processing unit in a polynomial sequence appending process wherein the encrypted user key is combined with a factory preset code key and wherein this secure key is decrypted by the data processing unit.

PATENTS • DESIGNS • The Patent Office • COPYRIGHT • TRADE MARKS

INVESTOR IN PEOPLE

Application No:	GB0423668.3	**Examiner:**	Michael Powell Waters
Claims searched:	1-3	**Date of search:**	10 December 2004

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X,E	3	GB 2387933 A (RITECH) see pages 5 and 6 and figure 3
X	3	EP 0673134 A2 (CANON) see whole document

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^{W} :

G4A

Worldwide search of patent documents classified in the following areas of the IPC^{07}

G06F; H04L

The following online and other databases have been used in the preparation of this search report

WPI, EPODOC, PAJ, INSPEC, XPESP, IP.COM, IEL, Internet, TDB